IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF HAWAII

UNITED STATES OF AMERICA)	MAG. NO. 03 03 0831
)	
v.)	APPLICATION AND AFFIDAVIT
)	FOR SEARCH WARRANT;
ONE COMPAQ SERIES PP2140)	ATTACHMENT "A";
LAPTOP COMPUTER,)	ATTACHMENT "B"
SERIAL NUMBER 9X2AKSBZN2E4,)	
AND ASSOCIATED PERIPHERALS AND)	
STORAGE MEDIA DESCRIBED MORE)	
FULLY IN ATTACHMENT "A")	
)	

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

The undersigned person, after being duly sworn, deposes and says that there is reason to believe that:

On the premises/property described in the attached Affidavit (which is hereinafter referred-to as "Affidavit" and incorporated herein by reference), in the District of Hawaii,

There is now concealed the property and materials identified in the Affidavit, which is property and materials that constitutes evidence of the commission of a criminal offense; contraband, the fruits of crime, or things otherwise criminally possessed; and property designed or intended for use or which is or has been used as the means of committing a criminal offense,

Concerning violations of Title 18, United States Code, Sections 13, 2242, 2252, and 2252A, and Hawaii Revised Statutes 711-1110.9.

//

//

//

//

//

The facts to support a finding of Probable Cause are set forth in the attached Affidavit.

AFFIANT'S NAME: MICHAEL E. WESTBERRY
AFFIANT'S POSITION: Special Agent
AFFIANT'S FED. LAW ENFORCEMENT AGENCY: U.S. Naval Criminal Investigative Service

Sworn to before me, and subscribed in my presence:

October 10, 2003, at Honolulu, Hawaii.

UNITED STATES MAGISTRATE JUDGE

AGENT'S AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, MICHAEL E. WESTBERRY, being duly sworn, depose and state as follows:

1. I am a Special Agent with the Department of the Navy, Naval Criminal Investigative Service, Pear Harbor, Hawaii. I have been a Special Agent with the Naval Criminal Investigative Service for approximately the last year. I have investigated matters involving Rape, Indecent Assault, Aggravated Assault, Possession and Distribution of Child Pornography over the Internet, as well as numerous other violations of the Uniform Code of Military Justice and Title 18 of the United States Code. I have conducted numerous searches pertaining to the investigation of these types of investigations.

2. I am the case agent assigned to investigate the activities of James Ronald GERVAIS ("GERVAIS") who is an active duty member of the United States Navy, stationed aboard the USS SALVOR (ASR 52), home ported at Naval Station Pearl Harbor, Hawaii. As is set forth below, there is probable cause to believe GERVAIS possesses materials including, but not limited to, computer files, disks, and digital media which constitute evidence of violations of Title 18 United States Code, Sections 13, 2242 and Hawaii Revised Statutes 711-1110.9. Additionally, there is probable cause to believe GERVAIS possesses images and depictions of minors engaging in sexually explicit conduct in violation of Title 18, United States Code, Sections 2252 and 2252A.

3. I am submitting this affidavit in support of a search warrant authorizing a search of GERVAIS' COMPAQ series PP2140 laptop computer, Serial Number 9X2AKSBZN2E4, and associated electromagnetic, digital, and compact laser disc media (collectively "GERVAIS computer") which items were seized from several locations including GERVAIS' barracks room, Oklahoma Hall, room 118, Naval Station Pearl Harbor, HI 96818 ("GERVAIS barracks room"), the USS SALVOR (ASR 52) docked at B17, Naval Station Pearl Harbor, HI 96818 ("USS SALVOR"), and GERVAIS' 1992 Ford Mustang ("GERVAIS Mustang") pursuant to a military Command Authorization for Search and Seizure dated October 1, 2003, and a Permissive Authorization for Search and Seizure.

4. This application seeks authority to search all computers, computer disks, compact laser disks ("CD's"), electromagnetic and other digital media seized from GERVAIS' barracks room, GERVAIS' Mustang, and the USS SALVOR, as set forth more fully in Attachment "A," for evidence of the forgoing violations.

5. Title 18, United States Code, Section 2242, prohibits knowingly causing another person to engage in a sexual act by threatening or placing that other person in fear, other than threatening or placing the other person in fear that any person will be subjected to death, serious bodily injury, or kidnapping.

6. Title 18, United States Code, Section 2252(a)(4), prohibits persons in the special maritime and territorial jurisdiction of the United States, or on any land or building owned by, leased to, or otherwise used by or under the control of the Government of the United States, or in the Indian country as defined in section 1151, from knowingly possessing 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction, if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct.

7. Title 18, United States Code, Section 2252A(5) prohibits persons in the special maritime and territorial jurisdiction of the United States, or on any land or building owned by, leased to, or otherwise used by or under the control of the Government of the United States, or in the Indian country as defined in section 1151, knowingly possessing any book, magazine, periodical, film, video tape, computer disk, or any other material that contains an image of child pornography.

8. The statements contained in this affidavit are based on my own investigative effort or, where indicated information provided by other law enforcement officers and witnesses. Since this affidavit is being provided for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts I believe necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. § 2242 (Sexual Abuse) and 18 U.S.C. § 2252 (Certain activities relating to material involving the sexual exploitation of minors), are located on GERVAIS' computer and associated electromagnetic, digital, and compact laser disk media.

DEFINITIONS

9. The term "Sexual act" is defined by 18 U.S.C. § 2246(2) as contact between the penis and the vulva or the penis and the anus. Contact involving the penis occurs upon penetration, however slight.

10. "Visual depictions" include undeveloped film and videotape, and data stored on computer disks or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

11. The term "computer," as used herein, is defined pursuant to Title 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

12. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

13. "Sexually Explicit Conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons.

14. "Child Erotica" are materials or items that are sexually arousing to pedophiles but that are not in and of themselves obscene or which do not necessarily depict minors in sexually explicit poses or positions. Child Erotica is defined as follows: "Any material, relating to children, that is sexually arousing to a given individual … Some of the more common types of child erotica include photographs that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids."

15. "Child Pornography," as used in this affidavit, includes the definition in 18 U.S.C. § 2256, as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct (see 18 U.S.C. § 2252).

16. "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address, which is used each time the computer accesses the Internet.

17. "URL" or "Uniform Resource Locator" refers to an Internet address. Each file on the Internet has a unique address called a Uniform Resource Locator, mote commonly known as URL.

SPECIFICS OF SEARCHES AND SEIZURES OF COMPUTER SYSTEMS

18. During the course of my investigation of GERVAIS' conduct, I consulted with an expert in computer searches, Investigative Computer Specialist Jamie Turner ("TURNER") of the Naval Criminal Investigative Service. According to TURNER, searching and seizing information from computers often requires agents to seize all electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environments. This is true because of the following:

a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, CD-ROMs, DVDs, and Bernoulli drives) can store the equivalent of hundreds of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence, and he might store criminal evidence in random order or with deceptive file names or deceptive file

extensions. This requires searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.

b. Searching computer systems for criminal evidence is a highly technical process, requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources and from destructive codes imbedded in the system, such as "booby traps"), a controlled environment is essential to its complete and accurate analysis.

19. Based upon my personal experience and consultation with experts in computer searches, data retrieval from computers and related media, and consultations with other agents who have been involved in the search of computers and retrieval of data from computer systems, your affiant knows that searching computerized information for evidence or instrumentalities of crime commonly requires agents to seize all of a computer system's input/output peripheral devices, related software, documentation, data security devices (including passwords), and any papers, correspondence, receipts or documents so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true because of the following:

a. The peripheral devices, which allow users to enter or retrieve data from the storage devices, vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output (or "1/0" devices in order to read the data on the system. It is important the analyst be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence contained therein. In addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers). And any applications software, which may have been

used to create the data (whether stored on hard drives, removable media or on external media), as well as all related instruction manuals or other documentation and data security devices. If the analyst determines that the I/O devices, software, documentation, and data security devices are not necessary to retrieve and preserve the data after inspection, the government will return them within a reasonable time.

b. In order to fully retrieve data from a computer system, the analyst also needs all magnetic storage devices as well as the central processing unit (CPU). Further, the analyst again needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software that may have been used to create the data (whether stored on hard drives or on external media) for proper data retrieval.

20. In addition, there is probable cause to believe that the computer and its storage devices, the monitor, keyboard, and modem are all instrumentalities of the crimes of receipt and possession of child pornography, in violation of law, and should all be seized.

USE OF COMPUTERS TO RECORD CRIMIAL ACTIVITY

21. As a result of my training and experience and the experience of other law enforcement personnel involved in this investigation, I know that video cameras, and digital still cameras, capable of recording in digital and analog formats can be used to record criminal activity for future viewing and as trophies of past accomplishments. Individuals who commit crimes communicate with their victims and store digital media used to control the actions of their victims utilize computers to accomplish their goals. Computers are also used to: a) correspond with like-minded individuals via e-mail, chat, bulletin boards, newsgroups, instant messages, file transfers and other means; b) store identifying information concerning victims, as well as identifying information about other individuals who share the same interests. Computers also afford individuals a degree of anonymity.

USE OF COMPUTERS WITH CHILD PORNOGRAPHY

22. As a result of my training and experience and the experience of other law enforcement personnel involved in this investigation, I know that computers are utilized by individuals who exploit children (which includes collectors of child

pornography), to: a) correspond with like-minded individuals via e-mail, chat, bulletin boards, newsgroups, instant messages, file transfers and other means; b) store identifying information concerning child victims, as well as identifying information about other- individuals who share the same interests; c) locate, view, download, collect and organize images of child pornography found through the Internet.

23. The Internet and its World Wide Web afford collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

24. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. These Online storage accounts are often free but can involve a charge. Payment is almost always made via credit card, debit card, or other similar payment service.

25. A subscriber assigned a free online storage account frequently can setup such accounts by providing limited identifying information. Any information provided is frequently fictitious in an attempt to preserve the anonymity of the user. Consequently, even if it is known that a collector or distributor of child pornography is a subscriber of a free online storage service, the service provider frequently will have no records in that subscriber's name. Instead, the Online service will only be able to identify files, including child pornography, that are associated with a "login name," or obscure, user created identity of the subscriber uses to "log on" to the online service.

26. Such an online storage account is particularly useful to a collector or distributor of child pornography. Such a subscriber can collect, store, view and distribute electronic images, including child pornography, directly from the Online service. Consequently, the illegal files have minimal contact with the subscriber's home computer. The subscriber can also manipulate the files on an online storage service from any computer connected to the Internet.

27. Nonetheless, evidence of an online storage account is often found on a home computer of a user subscribing to such a service. Evidence of an online storage account may take the form of passwords located in encrypted, archived or other files on the user's home computer. Other evidence can also be found through unique software that may exist on a user's home computer that has been developed by the online storage service. This unique software will frequently contain evidence not only of the existence of-such accounts, but the login and password.

28. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of ones favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. According to J. Turner, a forensic examiner often can recover evidence suggesting whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files, which were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

29. Based on my training and experience, together with the training and experience of the experts I have consulted and the corporate knowledge, training, and experience of other law enforcement officers involved in the investigation of child exploitation, pedophiles and collectors of child pornography demonstrate the following behavioral patterns:

a. Pedophiles are individuals whose sexual objects are children. Pedophiles receive sexual gratification and satisfaction from actual physical contact with children and from fantasies involving the use of pictures and/or photographic or art media depicting children. Such depictions range from fully clothed depictions of children engaged in non-sexual activity to nude or partially nude children engaged in sexual activity.

b. Pedophiles, being sexually attracted to children, collect sexually explicit materials involving

children, such as photographs, magazines, videotapes, books, slides and other computer images for their own sexual gratification. The most common method of acquiring the material is by trading the materials with other people with similar interests.

c. Since sex with children and the collection of child pornography is illegal, pedophiles desire privacy, anonymity, and a means to avoid detection by law enforcement. The use of computers by pedophiles to traffic, trade and collect child pornography and obscenity is a growing phenomenon. An individual familiar with computers can utilize the computer's ability to interact with many distant individuals while remaining largely hidden. This sense of privacy and secrecy along with the ability to interact with many individuals without risk of easy identification satisfies the needs of individuals who are interested in trafficking, trading and collecting child pornography.

d. Individuals involved in the collection of child pornography RARELY, IF EVER, dispose of their sexually explicit material. Such materials are instead treated as prized possessions, which can be viewed or traded over a long period of time. It is further unlikely that the condition of those items depicting the sexual exploitation of children will be altered or damaged from the original condition at the time of receipt based on the desire to keep the items in the original condition. Moreover, taken together, the increased sense of security which a computer affords and the known desire to retain child pornography and other prohibited obscenities for long periods provide probable cause to believe that computer images will be retained for as long as other types of child pornography. During the execution of numerous search warrants, law enforcement officers have found that pedophiles that store child pornography on their computers typically retain the images indefinitely.

e. Individuals involved in the sexual exploitation of children often collect books, magazines, newspapers, letters and other materials relating to children. Such individuals also collect other written material on the subject of sexual activities with children, which range from fantasy to medical, sociological, psychological and psychiatric writings. Such contact, correspondence or writings can and are now done by computer as well as through the use of mails or telephone. They rarely destroy these materials because of the psychological support and reinforcement they provide; the materials tend to validate each pedophile's interest by making

that person feel his/her interests are normal rather than deviant.

f. Individuals involved in the collection and distribution of child pornography almost always *maintain and* possess their materials in a place considered secure, most frequently within the privacy and security of their own homes. As discussed above, child pornography, obscenity or related materials may also be stored in a computer that may be additionally protected by passwords and other security devices.

g. Individuals who are procurers and distributors of child pornography contrary to law exhibit similar characteristics and will maintain their pictures, films, correspondence and photographs in a secure place, most often a residence, to avoid detection-by law-enforcement. It is also known by the affiant that child pornography is not lawfully available in retail establishments and that person(s) who wish to obtain child pornography do so by ordering it abroad or by discreet contact with other individuals who have it available.

h. Individuals who are involved with child pornography will often collect, read, copy or maintain numbers or lists of persons who have similar sexual interests. These contacts are maintained as a means of personal referral, exchange, and commercial profit. These names may be maintained in the original publication or mode of receipt, in phone books, notebooks, scraps of paper, or in computers.

i. Individuals who receive, transport, possess, and distribute child pornography, contrary to law, often keep records of their involvement with such activities, and these records include but are not limited to associate names and addresses, the identity and location of assets illegally gained through criminal activity, child erotica and material used to create, receive, transport, possess, distribute and sell child pornography.

FACTUAL BACKGROUND

30. This application for a search warrant authorizing a search of GERVAIS computer stems from a report to the Naval Criminal Investigative Service that Tsatoke LONEWOLF ("LONEWOLF") was sexually abused by GERVAIS while in his bed aboard a berthing barge adjacent to the USS SALVOR, docked at the Pier B17, Naval Station Pearl Harbor, Hawaii. The details of the investigation may be summarized as follows:

a. On October 1, 2003, at approximately 1600, GERVAIS provided a written sworn statement wherein he outlined his relationship with LONEWOLF.

b. In that statement, GERVAIS stated that he had been the roommate of LONEWOLF since July 2001 and shortly after became sexually and emotionally attracted to him. GERVAIS stated that he first had sex with LONEWOLF around December 2001, that LONEWOLF was a willing participant, and that he had sexual intercourse, both oral and anal, with LONEWOLF approximately 25 times over the period of approximately 18 months. GERVAIS further stated that he thought he and LONEWOLF were engaged in a mutual homosexual relationship, but that LONEWOLF terminated the relationship when he started dating a female.

c. GERVAIS admitted that he set up video camera equipment to surreptitiously film his sexual acts with LONEWOLF and that LONEWOLF had no knowledge of the videos. The surreptitiously recorded sexual act GERVAIS used to threaten LONEWOLF occurred within the special maritime and territorial jurisdiction of the United States. GERVAIS stated that LONEWOLF only became aware of the videos when GERVAIS used them to threaten LONEWOLF in order to extort sexual acts from him. According to GERVAIS, he showed LONEWOLF the computer files on his Compaq PP2140 series computer, depicting himself having sex with LONEWOLF, and told LONEWOLF he would release the computer file to the command if LONEWOLF did not have sex with him.

d. GERVAIS admitted he told LONEWOLF that if he did not continue his sexual relationship with him, GERVAIS would release the computer files to LONEWOLF's Commanding Officer and ruin his career. According to GERVAIS, LONEWOLF "gave in" and had sex with him because he did not want his command finding out he had previously had sex with a guy.

e. GERVAIS also stated that he had arranged video cameras in LONEWOLF's barracks room to film LONEWOLF and his girlfriend having sex without LONEWOLF's girlfriend's knowledge. GERVAIS further advised that he had purchased a spy camera and placed in a location to observe the shower in the bathroom he shared with LONEWOLF. He also stated that he did this as a joke and removed it when it was discovered.

f. GERVAIS stated that in April 2003, he reserved a room for himself and LONEWOLF at the Marriott hotel in Waikiki, HI. GERVAIS admitted he then threatened LONEWOLF

with the release of the video if LONEWOLF did not accompany him to the hotel and allow him to perform homosexual acts on him.

g. GERVAIS also stated that between September 23 and 30, 2003, he repeatedly offered LONEWOLF $2000.00 to spend "one last night" with him, and LONEWOLF repeatedly declined.

h. GERVAIS further advised that on October 1, 2003, he again tried to threaten LONEWOLF with the computer video, and that he tried to convince LONEWOLF to have one last sexual encounter with him. LONEWOLF declined, and left the barracks and returned to the berthing barge adjacent to the USS SALVOR. GERVAIS followed LONEWOLF to the berthing barge shortly thereafter, and the two began to argue about GERVAIS repeated sexual advances. During the argument, GERVAIS grabbed LONEWOLF's buttocks, at which point LONEWOLF became very angry and struck GERVAIS several times.

i. GERVAIS further stated that after the altercation in the berthing barge, he returned to his barracks room and placed his computer in his locker, and denied doing anything to LONEWOLF's car. However, shortly after the altercation LONEWOLF's vehicle was discovered with a key broken off in the ignition with the engine running, and the lug nuts on the right front tire loosened to cause the vehicle to lose control if driven.

j. Both GERVAIS and LONEWOLF advised your affiant that they corresponded via e-mail, using their official U.S. Navy e-mail accounts, regarding the facts and circumstances of this case. Based on that knowledge, your affiant requested and subsequently seized a zip-disk, # 130699A5AP, containing e-mail correspondence of both LONEWOLF and GERVAIS. That information was obtained from a U.S. Navy computer network, and provided at the direction and on the authority of the Commanding Officer, USS SALVOR (ASR 52).

k. After being sworn to his written statement, GERVAIS verbally admitted to possessing child pornography on his Compaq Presario laptop computer. GERVAIS subsequently gave a second written statement in which he stated his belief that the child pornography was included among other files on a CD-R given

to him by a co-worker, and that he was aware he had between "15 and 20" images of children "around ten years old" along with "one or two child pornography multimedia files" on his computer. GERVAIS stated he "just never got around to deleting" those files.

l. In his second written statement GERVAIS stated that his Compaq computer is Internet capable and that he had access to and used LONEWOLF's RoadRunner internet account. GERVAIS further stated that he has three e-mail accounts with various service providers under the usernames: clmustang69@hotmail.com, voodoo24@msm.com, and jamesg1977@aol.com.

32. On October 2, 2003, a Command Authorization for Search and Seizure was executed and GERVAIS' barracks room was searched for evidence pertaining to this investigation. During this search GERVAIS' laptop computer was found along with two video cameras, one pinhole spy camera, numerous videotapes and rolls of film, negatives and CDs. Some of the CD labels read as follows: "Toke & Christine Fucking," "my porn," three CDs labeled "porn," "me and toke." Command members recovered one grey Zip disk from Gervias workspaces. One CD without labeling was recovered from GERVAIS vehicle under a Permissive Authorization for Search and Seizure.

33. On October 1, 2003, LONEWOLF provided a written sworn statement wherein he provided the following details:

a. LONEWOLF stated he first met GERVAIS in August 2001 and the two became friends due to their common interests. LONEWOLF and GERVAIS were subsequently assigned to the same barrack room.

b. Approximately eight months becoming roommates, around July 2002, GERVAIS tried to make sexual advances toward him and LONEWOLF told him to stop. LONEWOLF stated he informed GERVAIS that he was not homosexual, and the two came to an agreement that they would remain friends.

c. LONEWOLF then stated that about a week after that incident, he returned to his room drunk and passed out in his bed. About two months later, around September 2002, GERVAIS confronted LONEWOLF with a computer video depicting GERVAIS

performing oral sex on him and told him that he is going to get what he wants. LONEWOLF stated the video GERVAIS used to threaten him was made without LONEWOLF's knowledge or consent and that he has no recollection of the events depicted due to being blacked out from alcohol use.

d. LONEWOLF then stated he thereafter tried to avoid being in the room with GERVAIS and pretended that the incident depicted in the video never happened. LONEWOLF stated that he told GERVAIS to get rid of the videos, but GERVAIS told him that they were for his own personal use and that know one else would ever see them.

e. LONEWOLF stated that in late 2002 he discovered that GERVAIS had placed a pinhole spy camera in the shower and he told GERVAIS to remove it, and he did.

f. LONEWOLF advised that around December 2002 GERVAIS again confronted him with the videos of GERVAIS performing oral sex on him without his knowledge or consent and told LONEWOLF that if he did not accompany him to the Waikiki Marriott, and let GERVAIS perform oral sex on him, that GERVAIS would release the videos to his commanding officer and ruin his career. LONEWOLF also said that GERVAIS told him that he would destroy the videos if went to the hotel.

g. LONEWOLF stated that he went to the Waikiki Marriott with GERVAIS and allowed GERVAIS to perform oral sex on him to prevent the videos from being released to LONEWOLF's Navy command and in the hopes that they would be destroyed. However, LONEWOLF stated that the videos were not destroyed and between the time of the incident at the hotel and the assault on October 1, 2003, GERVAIS continued to threaten him with the videos in an effort to extort additional sexual acts from LONEWOLF.

h. LONEWOLF stated that on the morning of October 1, 2003, he arrived at his barracks room around 0330 and that GERVAIS again started making sexual advances toward him. LONEWOLF left the barracks room to go to the berthing barge and get some sleep. While in a rack onboard the berthing barge, GERVAIS arrived and again made sexual advances toward him. LONEWOLF stated that GERVAIS on several occasions attempted to reach for his crotch area and again threatened that if he did not allow GERVAIS to perform oral sex on him that GERVAIS would release the video to the entire crew of the USS SALVOR.

i. LONEWOLF stated that during this conversation, GERVAIS also threatened to damage his car and kill his girlfriend. LONEWOLF also stated that GERVAIS again tried to show him the computer screen depicting GERVAIS performing oral sex on him, and again attempted to reach for LONEWOLF's crotch area. It was at this time that LONEWOLF exited his rack and punched GERVAIS, who then departed the area with his computer.

WHEREFORE, based upon the foregoing, I believe that there is probable cause to believe that on the GERVAIS' laptop computer and associated computer and photographic media, storage media, and peripherals more particularly described in Attachment "A" hereto, there are presently located the items specified in Attachment "B" hereto, which items constitute evidence of the commission of criminal offenses, namely, violations of 18 U.S.C. §§ 13, 2242, and Hawaii Revised Statutes 711-1110.9, and materials held in violation of 18 U.S.C. § 2252 and 2252A, contraband, the fruits of crimes, things otherwise criminally possessed, and property which is or has been used as the means of committing the foregoing offenses.

DATED: October 10, 2003, at Honolulu, Hawaii.

FURTHER AFFIANT SAYETH NAUGHT.

MICHAEL E. WESTBURY, Special Agent
U.S. Naval Criminal Investigative Service

Sworn and Subscribed before me
this 10th day of October, 2003:

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT "A"

LIST OF ITEMS TO BE SEARCHED

Items seized from James Ronald GERVAIS' barracks room # 118, building 900, Oklahoma Hall, Naval Station Pearl Harbor, HI 96818, GERVAIS' Ford Mustang, and the USS SALVOR including:

1. Compaq Presario laptop computer, S/N 9X2AKSBZN2E4;
2. One Fossil Data Bank Digital Calendar;
3. One Imation 3 ½" disk labeled "EM3 Gervais";
4. One Memorex CD-RW last 4 S/N 9753;
5. One IOmega Zip disk S/N 21F082ACP;
6. One IOmega Zip disk S/N 120501A4BP;
7. Two VHS Video tapes with one labeled "Porn", one nlabeled;
8. One JVC VHSC tape;
9. One C-P7U cassette adaptor initials "ARS10-1-03" containing one JVC VHSC tape;
10. One "Sprint" camera phone bearing the initials "ARS";
11. One "Kodak Max" disposable camera S/N 061218;
12. One "Sony Cybershot" digital camera S/N 387673 and associated memory stick;
13. One Imation CD-R last 4 S/N 0076, one Imation CD-R last 4 S/N 0080 and labeled "Good slow songs";
14. One Imation CD-R last 4 S/N 0077 labeled "Foreigner and Moby";
15. One Imation CD-R last 4 S/N 2927 labeled "Lil kim";
16. One Imation CD-R last 4 S/N 0075 labeled "The black crowes";
17. One Fujifilm CD-R last 4 S/N 6980;
18. One Imation CD last 4 S/N 1485 labeled "Songs for toke";
19. One Imation CD-R last 4 S/N 1489 labeled "my porn";
20. One Imation CD-R last 4 S/N Z931 labeled "my porn";
21. One Imation CD-R last 4 S/N 1488 "me and toke";
22. One Imagion CD-R last 4 S/N 6107;
23. One Imation CD-R last 4 S/N 0073 with illegible writing;
24. One Imation CD-R last 4 S/N 6107;
25. One Imation CD-R last S/N 22LHD5;
26. One CD last 4 S/N RA08 labeled "Carat 2002 Cruise CD";
27. One Imation CD-R last 4 S/N 1484 labeled "Songs for toke II";
28. One Imation CD-R last 4 S/N 2932 labeled "Good songs";
29. One CD-R last 4 S/N LHD1;
30. One Fujifilm CD-R last 4 S/N 1780;

31. One Imation CD-R last 4 S/N 1541;
32. One CD last 4 S/N Q400;
33. One Fujifilm CD-R last 4 S/N 4980;
34. One Imation CD-R last 4 S/N 0071 with illegible writing;
35. One Imation CD-R last 4 S/N 0074 labeled "Tracy chapman and stuff";
36. One Imation CD-R last 4 S/N 0913 P
37. One CD container with 16 unlabeled CD's;
38. One Fujifilm Zip disk S/N 21A071ABP;
39. One Fujifilm CD-R labeled "Chris and toke fucking";
40. One Imation DVD+R last 4 S/N D016;
41. One Imation DVD+R last 4 S/N C016;
42. One Imation DVD-R last 4 S/N A016;
43. One Sony Handy Cam S/N 106751 and associated tape;
44. One TDK MP120 labeled "mac richard";
45. One Sony Hi8 MP120 "Both on our trip to chicago";
46. One unlabeled Hi8 MP120 tape;
47. One Maxell 8mm MP labeled "underway from thailand";
48. One TDK HG tape # AHFJ102;
49. One TDK HG tape # AHFJ102;
50. One JVC tape # 3AE06;
51. One JVC tape # WC-S2Q6;
52. One JVC tape # WC-LQQ6
53. One Imation CD-R last 4 S/N 2936;
54. One zip disk, S/N 130699A5AP.

ATTACHMENT "B"

LIST OF ITEMS TO BE SEIZED

1. All materials, in whatever form, media, or format, including computer files, prints, videos, videotapes, photographs, negatives, magazines, and books, which contain child pornography, child erotica, the visual depictions of minors engaged in sexually explicit conduct, as well as materials depicting, purporting to depict, or pertaining to violations of 18 U.S.C. §§ 13, 2242, 2252, 2252A and Hawaii Revised Statutes 711-1110.9.

2. Any and all computer software, including programs to run operating systems, applications (like word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications program.

3. Any computer-related documentation, which consists have written, recorded, printed or electronically stored material that explains or illustrates how to configure or use computer hardware, software or other related items.

4. Any and all records and materials, in whatever form, media, or format (including, but not limited to, envelopes, letters, papers, e-mail, chat logs and electronic messages, other digital data files and web cache information) a) pertaining to the possession, receipt or distribution of child pornography or the visual depictions of minors engaged in sexually explicit conduct; b) pertaining to the manufacture, possession, receipt or distribution of materials and images depicting violations of 18 U.S.C. § 13, 2242 or Hawaii Revised Statutes 711-1110.9, c) identifying persons transmitting through interstate or foreign commerce, including via computer, any child pornography or visual depiction of minors engaged in sexually explicit conduct; or d) bearing on the receipt, shipment or possession of child pornography or the visual depictions of minors engaged in sexually explicit conduct.

5. Records of communication (as might be found, for example, in digital or electronic data files) between individuals concerning the topic of child pornography, the existence of sites on the Internet that contain child pornography or which cater to those with an interest in child pornography, as well as evidence Of membership in online clubs, groups, services, or other Internet sites that provide or make accessible child pornography to its members and constituents.

6. Records of communication (as might be found, for example, in digital or electronic data files) between individuals concerning or pertaining to violations of 18 U.S.C. § 13, 2242 or Hawaii Revised Statutes 711-1110.9.

7. Evidence of association, by use, subscription or free membership, with Online clubs, groups, services, or other Internet sites that provide or otherwise make accessible child pornography.

8. Evidence of any online storage, e-mail or other remote computer storage subscription to include unique software of such subscription, user logs or archived data that show connection to such service, and user login and passwords for such service.

9. Items of personal-property and other evidence tending to identify the person(s) in control or ownership of the computer and other electronic media authorized to be searched by this warrant (as set forth more fully in Attachment "A"), including but not limited to letters, correspondence, canceled mail, deeds, leases, rental agreements, photographs, personal telephone books, diaries, utility and telephone bills.

10. Records or other items, in whatever form, media, or format evidencing ownership or use of computer equipment and paraphernalia authorized to be searched by this warrant (as set forth more fully in Attachment "A"), including, but not limited to, sales receipts, registration records, records of payment for Internet access, records of payment for access to newsgroups or other online subscription services, handwritten notes and handwritten notes, e-mail messages, and computer files.